# Decoding method for generalized algebraic geometry codes*

Ryutaroh Matsumoto Masakuni Oishi†
ryutaroh@rmatsumoto.org
Department of Communications and Integrated Systems
Tokyo Institute of Technology, 152-8552 Japan

April 24, 2001

**Abstract**

We propose a decoding method for the generalized algebraic geometry codes proposed by Xing et al. To show its practical usefulness, we give an example of generalized algebraic geometry codes of length 567 over $\mathbf{F}_8$ whose numbers of correctable errors by the proposed method are larger than the shortened codes of the primitive BCH codes of length 4095 in the most range of dimension.

## 1 Introduction

Recently Xing, Niederreiter and Lam [11] introduced a construction of linear codes from algebraic function fields and places of degrees larger than one. They call their new construction *generalized algebraic geometry codes*, which is a generalization of functional algebraic geometry codes first explicitly defined in [6, 9]. The lower bound for the minimum distance by Xing et al. was improved by Özbudak and Stichtenoth [8].

Nobody has proposed a decoding method that corrects errors up to half the designed minimum distance by Özbudak and Stichtenoth. We give a

*This paper is registered at the LANL eprint server http://arXiv.org/.
†All correspondence should be sent to the first author.

decoding method that corrects errors almost half the designed minimum distance.

Although several examples were given [11], the usefulness of generalized algebraic geometry codes has not been clearly demonstrated. We give an example of generalized algebraic geometry codes whose numbers of correctable errors by the proposed method are larger than the shortened codes of BCH codes of the same dimension (see Fig. 1).

It should be noted that Kaida et al. [5] also considered a code construction using places of degree larger than one, which is a special case of generalized algebraic geometry codes. However, they gave neither lower bound for the minimum distance nor interesting example.

# 2 Notations

Let us fix notations used in this paper. We shall always consider linear codes over the finite field $\mathbf{F}_q$ with $q$ elements. Notations follow those in Stichtenoth's textbook [10]. Let $F/\mathbf{F}_q$ be an algebraic function field of one variable over the full constant field $\mathbf{F}_q$. Let $P_1, \ldots, P_s$ be pairwise distinct places of $F/\mathbf{F}_q$, not necessarily of degree one. Let $G$ be a divisor of $F/\mathbf{F}_q$ whose support contains none of $P_1, \ldots, P_s$.

For ease of presentation we shall define a subclass of generalized algebraic geometry codes in a slightly different manner from the original [11]. Let $m$ be the least common multiple of $\deg P_1, \ldots, \deg P_s$. Let $\tilde{F} = F\mathbf{F}_{q^m}$, that is, the constant field extension of $F$. Let $\tilde{P}_{i,1}, \ldots, \tilde{P}_{i,\deg P_i}$ be the extensions of $P_i$ in $\tilde{F}/F$. The residue class field $O_{P_i}/P_i$ can be regarded as a subfield of $O_{\tilde{P}_{i,1}}/\tilde{P}_{i,1}$ via the $\mathbf{F}_q$-embedding $\iota_i$ sending $(x \bmod P_i) \in O_{P_i}/P_i$ to $(x \bmod \tilde{P}_{i,1}) \in O_{\tilde{P}_{i,1}}/\tilde{P}_{i,1}$. Let $\iota_i(F_{P_i})$ be the image of $F_{P_i} = O_{P_i}/P_i$ under $\iota_i$. We have the field isomorphism

$$\iota_i(F_{P_i}) \simeq \mathbf{F}_{q^{\deg P_i}}. \tag{1}$$

Let $\pi_i$ be an $\mathbf{F}_q$-linear isomorphism from $\iota_i(F_{P_i})$ to $\mathbf{F}_q^{\deg P_i}$. We shall consider the generalized algebraic geometry code defined by

$$C = \{(\pi_1(f(\tilde{P}_{1,1})), \pi_2(f(\tilde{P}_{2,1})), \ldots, \pi_s(f(\tilde{P}_{s,1}))) \mid f \in \mathcal{L}(G)\},$$

where $\mathcal{L}(G)$ is $\{f \in F \mid \text{the principal divisor of } f \geq -G\}$. The length of $C$ is given by $n = \deg P_1 + \cdots + \deg P_s$. The dimension of $C$ is given by $\dim G - \dim(G - (P_1 + \cdots + P_s))$.

In the original definition of generalized algebraic geometry codes [11], $\pi_i$ is defined as an injective $\mathbf{F}_q$-linear map from $F_{P_i}$ to $\mathbf{F}_q^{\gamma_i}$, where $\gamma_i$ is an integer $\geq \deg P_i$. Our definition is equivalent to the case of $\gamma_i = \deg P_i$.

# 3 Decoding method

In this section we propose a decoding method for $C$ using a decoding method for a code over $\mathbf{F}_{q^m}$.

The field $\iota_i(F_{P_i})$ is isomorphic to $\mathbf{F}_q^{\deg P_i}$ as an $\mathbf{F}_q$-space. We shall consider the $\mathbf{F}_q$-space

$$\tilde{C} = \{(f(\tilde{P}_{1,1}), f(\tilde{P}_{2,1}), \ldots, f(\tilde{P}_{s,1})) \mid f \in \mathcal{L}(G)\}$$

that can be regarded as an $\mathbf{F}_q$-subspace of

$$\Lambda = \mathbf{F}_{q^{\deg P_1}} \times \mathbf{F}_{q^{\deg P_2}} \times \cdots \times \mathbf{F}_{q^{\deg P_s}}$$

by isomorphisms (1).

For an array $\boldsymbol{x} = (x_1, \ldots, x_s)$, where $x_i$ is an element in some field, we define the Hamming weight of $\boldsymbol{x}$ to be the number of nonzero component in $\boldsymbol{x}$.

Let $\sigma$ be the Frobenius automorphism of $\mathbf{F}_{q^m}$ sending $\alpha$ to $\alpha^q$. $\sigma$ can be extended to the automorphism of $\tilde{F}/F$ in a natural manner. We may assume $\sigma\tilde{P}_{i,j} = \tilde{P}_{i,j+1}$ without loss of generality [10, Theorem III.7.1].

We define the following $\mathbf{F}_q$-spaces:

$$\begin{aligned} \Lambda_{\text{ex}} &= \mathbf{F}_{q^{\deg P_1}}^{\deg P_1} \times \mathbf{F}_{q^{\deg P_2}}^{\deg P_2} \times \cdots \times \mathbf{F}_{q^{\deg P_s}}^{\deg P_s}, \\ \tilde{C}_{\text{ex}} &= \{(f(\tilde{P}_{1,1}), f(\tilde{P}_{1,2}), \ldots, f(\tilde{P}_{1,\deg P_1}), f(\tilde{P}_{2,1}), \ldots, f(\tilde{P}_{s,\deg P_s})) \mid f \in \mathcal{L}(G)\}. \end{aligned}$$

By isomorphisms (1), $\tilde{C}_{\text{ex}}$ can be regarded as an $\mathbf{F}_q$-subspace of $\Lambda_{\text{ex}}$.

For $f \in F$ with $v_{P_i}(f) \geq 0$, we have $\sigma(f(\tilde{P}_{i,j})) = (\sigma f)(\sigma\tilde{P}_{i,j}) = f(\sigma\tilde{P}_{i,j})$ [10, Proof of Lemma III.5.2 (c)]. So we have $(f(\tilde{P}_{1,1}), f(\tilde{P}_{1,2}), \ldots, f(\tilde{P}_{1,\deg P_1}), f(\tilde{P}_{2,1}), \ldots, f(\tilde{P}_{s,\deg P_s})) = (f(\tilde{P}_{1,1}), \sigma(f(\tilde{P}_{1,1})), \ldots, \sigma^{\deg P_1 - 1}(f(\tilde{P}_{1,1})), f(\tilde{P}_{2,1}), \ldots, \sigma^{\deg P_s - 1}(f(\tilde{P}_{s,\deg P_s})))$.

Consider an $\mathbf{F}_q$-linear map $\varphi : \Lambda \to \Lambda_{\text{ex}}$ sending $(x_1, \ldots, x_s)$ to $(x_1, \sigma x_1, \ldots, \sigma^{\deg P_1 - 1}x_1, x_2, \sigma x_2, \ldots, \sigma^{\deg P_s - 1}x_s)$. Then $\varphi$ is injective and $\varphi(\tilde{C}) = \tilde{C}_{\text{ex}}$.

Let $\mathrm{Con}_{\tilde{F}/F}(G)$ be the conorm of $G$ in $\tilde{F}/F$ [10, Definition III.1.8], then $\mathcal{L}(G)$ is an $\mathbf{F}_q$-subspace of $\mathcal{L}(\mathrm{Con}_{\tilde{F}/F}(G))$ [10, Theorem III.6.3 (d)]. Thus $\tilde{C}_{\mathrm{ex}}$ is a subcode of the ordinary algebraic geometry code

$$\tilde{C}_{\mathrm{ord}} = \{f(\tilde{P}_{1,1}), f(\tilde{P}_{1,2}), \ldots, f(\tilde{P}_{s,\deg P_s}) \mid f \in \mathcal{L}(\mathrm{Con}_{\tilde{F}/F}(G))\}.$$

Suppose that a codeword $\boldsymbol{c} \in C$ is sent and $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e} \in \mathbf{F}_q^n$ is received. Let $\pi$ be an $\mathbf{F}_q$-linear map from $\Lambda$ to $\mathbf{F}_q^n$ defined by $\pi_1 \times \cdots \times \pi_s$. When the number of errors is not too large, we can find $\varphi(\pi^{-1}(\boldsymbol{c}))$ from $\varphi(\pi^{-1}(\boldsymbol{r}))$ by using a decoding algorithm for $\tilde{C}_{\mathrm{ord}}$. We shall analyze the number of correctable errors by a $t$-error correcting algorithm for $\tilde{C}_{\mathrm{ord}}$.

We shall relate the Hamming weight of $\boldsymbol{x}$ in $\Lambda$ and $\varphi(\boldsymbol{x})$ in $\Lambda_{\mathrm{ex}}$. We define $\nu_i = \sharp\{j \mid \deg P_j = i\}$, where $\sharp$ denotes the number of elements in a set, and $\mu = \max\{\deg P_i \mid i = 1, \ldots, s\}$.

**Proposition 1** *Suppose that*

$$\sum_{i=a}^{\mu} i\nu_i \le w(\varphi(\boldsymbol{x})) < \sum_{i=a+1}^{\mu} i\nu_i, \tag{2}$$

*where $\boldsymbol{x} \in \Lambda$, and $w(\cdot)$ denotes the Hamming weight of $\cdot$. Then we have*

$$\begin{aligned} w(\boldsymbol{x}) &\ge \min\{\sharp S \mid S \subseteq \{1, \ldots, s\}, \sum_{i \in S} \deg P_i \ge w(\varphi(\boldsymbol{x}))\} \qquad (3) \\ &= \left\lceil \frac{w(\varphi(\boldsymbol{x})) - \sum_{i=a+1}^{\mu} (i-a)\nu_i}{a} \right\rceil. \end{aligned}$$

*Proof.* Let $\boldsymbol{x} = (x_1, \ldots, x_s)$. If $x_i \neq 0$ then $\sigma^j x_i \neq 0$ for any $j$. It follows that

$$w(\varphi(\boldsymbol{x})) = \sum_{x_i \neq 0} \deg P_i.$$

Thus we have

$$\begin{aligned} w(\boldsymbol{x}) &\ge \min\{\sharp S \mid S \subseteq \{1, \ldots, s\}, \sum_{i \in S} \deg P_i = w(\varphi(\boldsymbol{x}))\} \\ &\ge \min\{\sharp S \mid S \subseteq \{1, \ldots, s\}, \sum_{i \in S} \deg P_i \ge w(\varphi(\boldsymbol{x}))\}. \end{aligned}$$

We may assume $\deg P_1 \ge \cdots \ge \deg P_s$ without loss of generality. Define $\ell$ by

$$\sum_{i=1}^{\ell-1} \deg P_i < w(\varphi(\boldsymbol{x})) \le \sum_{i=1}^{\ell} \deg P_i.$$

We can easily see

$$\ell = \min\{\sharp S \mid S \subseteq \{1, \dots, s\}, \sum_{i \in S} \deg P_i \geq w(\varphi(\boldsymbol{x}))\}.$$

By the definitions of $a$ and $\ell$, we have $a = \deg P_\ell$, and

$$\begin{aligned} \ell &= \sum_{i=a+1}^{\mu} \nu_i + \left\lceil \frac{w(\varphi(\boldsymbol{x})) - \sum_{i=a+1}^{\mu} i\nu_i}{a} \right\rceil \\ &= \left\lceil \frac{w(\varphi(\boldsymbol{x})) - \sum_{i=a+1}^{\mu} (i-a)\nu_i}{a} \right\rceil. \end{aligned}$$ ■

**Theorem 2** *When we have a $t$-error correcting algorithm for $\tilde{C}_{\mathrm{ord}}$, we can correct up to*

$$\left\lceil \frac{t+1-\sum_{i=a+1}^{\mu}(i-a)\nu_i}{a} \right\rceil - 1$$

*errors of $C$, where $a$ is defined by*

$$\sum_{i=a}^{\mu} i\nu_i \leq t+1 < \sum_{i=a+1}^{\mu} i\nu_i.$$

*Proof.* Suppose that we sent $\boldsymbol{c} \in C$ and received $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e} \in \mathbf{F}_q^n$. By using the $t$-error correcting algorithm for $\tilde{C}_{\mathrm{ord}}$, we try to find $\varphi(\pi^{-1}(\boldsymbol{c}))$ from $\varphi(\pi^{-1}(\boldsymbol{r}))$, and compute $\boldsymbol{c}$ from $\varphi(\pi^{-1}(\boldsymbol{c}))$. In order for this method to work, it is sufficient that $w(\varphi(\pi^{-1}(\boldsymbol{e}))) \leq t$. We shall show that if $w(\boldsymbol{e}) \leq \lceil (t+1-\sum_{i=a+1}^{\mu}(i-a)\nu_i)/a \rceil - 1$ then $w(\varphi(\pi^{-1}(\boldsymbol{e}))) \leq t$.

We have $w(\boldsymbol{e}) \geq w(\pi^{-1}(\boldsymbol{e}))$. Suppose that $w(\varphi(\pi^{-1}(\boldsymbol{e}))) = t+1$. Then by Proposition 1

$$w(\boldsymbol{e}) \geq \left\lceil \frac{t+1-\sum_{i=a+1}^{\mu}(i-a)\nu_i}{a} \right\rceil, \tag{4}$$

which is a contradiction. Suppose that $w(\varphi(\pi^{-1}(\boldsymbol{e}))) > t+1$. Then the right hand side of Eq. (4) increases and the same contradiction is deduced. ■

**Remark 3** *Decoding algorithms for the functional algebraic geometry code $\tilde{C}_{\mathrm{ord}}$ are proposed in* [1, 2, 4, 7]. *In* [7] *the Feng-Rao decoding algorithm* [3] *is modified for functional algebraic geometry codes. Note that we have to represent $\tilde{C}_{\mathrm{ord}}$ as a residue algebraic geometry code before applying the algorithms* [1, 2], *and the algorithms* [4, 7] *are applicable only for one-point codes.*

**Remark 4** *Özbudak and Stichtenoth* [8] *showed that the minimum distance of $\tilde{C}$ is not less than*

$$\min\{\sharp S \mid S \subseteq \{1, \ldots, s\}, \sum_{i \in S} \deg P_i \geq n - \deg G\}. \tag{5}$$

*By an argument similar to the proof of Proposition* 1, *one can prove that the lower bound* (5) *is equal to*

$$\left\lceil \frac{n - \deg G - \sum_{i=a+1}^{\mu}(i-a)\nu_i}{a} \right\rceil,$$

*where $a$ is defined by*

$$\sum_{i=a}^{\mu} i\nu_i \leq n - \deg G < \sum_{i=a+1}^{\mu} i\nu_i.$$

**Remark 5** *In order to make the number of correctable errors and the lower bound* (5) *larger, we have to make the right hand side (RHS) of Eq.* (3) *larger. The RHS of Eq.* (3) *takes the maximum value for a fixed code length $n$ and $w(\varphi(\boldsymbol{x}))$ when the places $P_1, \ldots, P_s$ are of the smallest degrees.*

# 4 Examples

## 4.1 Good example

In this subsection we compare generalized algebraic geometry codes and BCH codes of length 567 over $\mathbf{F}_8$. We construct codes from the rational function field $\mathbf{F}_8(x)/\mathbf{F}_8$. We take $D$ as the sum of 7 places of degree 1, 28 places of degree 2, and 168 places of degree 3. We compare these generalized algebraic geometry codes with shortened codes of primitive BCH codes of length 4095. For each number of check symbols, we take a BCH code that has the largest BCH bound. The number of check symbols and the number of correctable errors of these codes are plotted in Fig. 1.

## 4.2 Bad example

In this subsection we give an example of generalized algebraic geometry codes with which we cannot correct errors up to half the designed minimum distance. Consider the rational function field $\mathbf{F}_{17}(x)/\mathbf{F}_{17}$. Take $D$ as the sum of

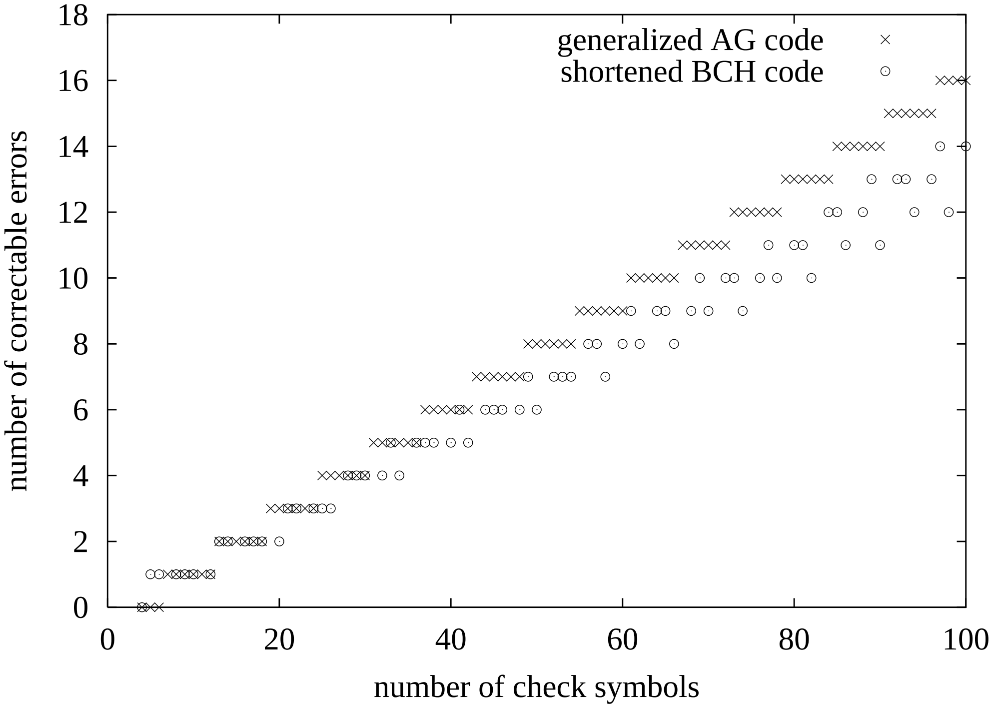


Figure 1: Comparison of generalized AG codes and BCH codes

17 places of degree 1 and a place of degree 4, and $G$ as a divisor of degree 13. Then the designed minimum distance is 5, while the number of correctable errors is 0.

## Acknowledgment

We would like to thank Prof. Tomohiko Uyematsu for helpful comments.

## References

[1] I. M. Duursma. Majority coset decoding. *IEEE Trans. Inform. Theory*, 39(3):1067–1070, May 1993.

[2] J. I. Farrán. Decoding algebraic geometry codes by a key equation. *Finite Fields Appl.*, 6(3):207–217, July 2000, `arXiv:math.AG/9910151`.

[3] G. L. Feng and T. R. N. Rao. Decoding algebraic geometric codes up to the designed minimum distance. *IEEE Trans. Inform. Theory*, 39(1):36–47, Jan. 1993.

[4] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Trans. Inform. Theory*, 45(4):1757–1767, Sept. 1999.

[5] T. Kaida, K. Imamura, and T. Moriuchi. A note on algebraic geometric codes with high degree places. In *Proc. 18th Symposium on Information Theory and Its Applications*, pages 231–234, Hanamaki, Japan, Oct. 1995 (Japanese).

[6] J. H. van Lint and T. A. Springer. Generalized Reed-Solomon codes from algebraic geometry. *IEEE Trans. Inform. Theory*, IT-33(3):305–309, May 1987.

[7] R. Matsumoto and S. Miura. On the Feng-Rao bound for the $\mathcal{L}$-construction of algebraic geometry codes. *IEICE Trans. Fundamentals*, E83-A(5):926–930, May 2000.

[8] F. Özbudak and H. Stichtenoth. Constructing codes from algebraic curves. *IEEE Trans. Inform. Theory*, 45(7):2502–2505, Nov. 1999.

[9] H. Stichtenoth. Self-dual Goppa codes. *J. Pure Appl. Algebra*, 55:199–211, 1988.

[10] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin, 1993.

[11] C. Xing, H. Niederreiter, and K. Y. Lam. A generalization of algebraic-geometry codes. *IEEE Trans. Inform. Theory*, 45(7):2498–2501, Nov. 1999.